Security Questionnaire

Updated: June 2022

Asset number: 0001322

Instructions

Use this questionnaire as a starting point for documenting important technical information that will assist with security policy and solution design, security policies, and security compliance. Work with your security team to add the information required for your environment.

Security Questionnaire

| **Question** | **Yes** | **No** | **Notes** |
| --- | --- | --- | --- |
| 1. **Access control** | | | |
| Will authentication mechanisms be required? |  |  |  |
| Is multi-factor enabled? |  |  |  |
| Are [Access-Control Lists](https://docs.servicenow.com/bundle/sandiego-platform-administration/page/administer/contextual-security/concept/access-control-rules.html) (ACL) and role-based access control (RBAC) in place? |  |  |  |
| Are there currently settings not enabled by default based on usage context? |  |  |  |
| Is there anti-virus protection in place? |  |  |  |
| Are the additional access control technical policies and security standards in place? |  |  |  |
| 1. **Email security** | | | |
| I have reviewed the email security policies. |  |  |  |
| Is anti-malware scanning in place? |  |  |  |
| Are our email filters in place? |  |  |  |
| Is an email domain restriction created? |  |  |  |
| Will email domain restrictions need to be customized? |  |  |  |
| Will whitelist email filters need to be created? |  |  |  |
| Is email security being monitored? |  |  |  |
| Are owners assigned to analyze metrics on spam, external emails, and inbound emails? |  |  |  |
| Is encryption in place (if the server accepts TLS)? |  |  |  |
| Is advanced email configuration implemented? |  |  |  |
| Are the additional email technical policies and security standards in place? |  |  |  |
| 1. **Logging and monitoring** | | | |
| Are there currently policies in place regarding logging and monitoring policies? |  |  |  |
| Will a plan be required to monitor application and event logs to highlight suspicious activity? (Note: Including the event log, system log, transaction logs, table auditing, record history, log archival, and browser SQL error messages) |  |  |  |
| Will table auditing be required for sensitive data? |  |  |  |
| Are additional logging and monitoring technical policies and security standards in place? |  |  |  |
| 1. **Encryption** | | | |
| Are encryption policies in place? (Note: Look at protected sensitive database fields or attachments with platform encryption including data in transit, data at rest, and integration traffic.) |  |  |  |
| 1. **Data security** | | | |
| Is data separation in place? |  |  |  |
| Is data tokenized? |  |  |  |
| Are there particular standards required based on industry or legal requirements (i.e., ISO standards for the database)? |  |  |  |
| Are there other data security policies and security standards in place? |  |  |  |
| 1. **Mobile application security** | | | |
| Are [Mobile-Specific Security Controls](https://docs.servicenow.com/csh?topicname=sg-mobile-security) are in place? |  |  |  |
| Is application preference the only record data stored on the mobile device? |  |  |  |
| Will additional controls be required? (i.e., mobile-specific system properties, attachment control, password reinforcement, security patching, and controlling shared data.) |  |  |  |
| Is data in transit protected with TLS and application preference information encrypted with AES128? |  |  |  |
| Are the additional mobile application technical policies and security standards in place? |  |  |  |
| 1. **Additional considerations** | | | |
| Will there be a review of [Instance Hardening Settings](https://docs.servicenow.com/bundle/sandiego-platform-administration/page/administer/security/reference/instance-security-hardening-settings.html) on the docs' page? |  |  |  |
| Will there be a review of the [ServiceNow Security Best Practice Guide](https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/success/playbook/instance-security-best-practice.pdf)? |  |  |  |
| Will there be a review of testing standards? |  |  |  |
| Is penetration testing a requirement? |  |  |  |
| Are there upgrade guidelines? |  |  |  |